

IN THE CLAIMS:

Claims 1-26 (canceled).

Please cancel claims 27-42, without prejudice, and insert in lieu thereof new claims 53-68.

Please cancel non-elected claims 43-52.

53. (new): Method to check the integrity and the authenticity of a data set received by a pay television decoding unit including a decoder, a security unit, and means of communication with a control center, comprising a first step of calculation by said decoding unit of a check information which is representative of the result of a unidirectional and collision-free function, carried out on all or part of the data set, said method comprising further steps of:

- transmitting the check information by said decoding unit to the security unit and ciphering said check information with a first cipher-key,
- sending the ciphered check information to the control center,
- deciphering of the ciphered check information by the control center and comparison with a reference value of the check information,
- transmitting control data including the result of the comparison in a ciphered form to the security unit,
- deciphering of the ciphered result of the comparison by the security unit and informing the decoder of the validity of the data set.

54. (new): The method according to claim 53, wherein the control center returns, in the control data, the reference value of the check information in a ciphered form to the security unit.

55. (new): The method according to claim 54, wherein the calculation is carried out by the decoder, the result of said calculation being transmitted to the security unit.

56. (new): The method according to claim 53, wherein the calculation is carried out by the security unit, the data set being transmitted from the decoder to the security unit.

57. (new): The method according to claim 53 comprising the further steps of:

- including an utilization describer for the data set in the control data,
- deciphering the control data and transmitting said describer to the decoder,
- if the result of the comparison is positive, processing the data set by the decoder according to guidelines contained in said describer.

58. (new): The method according to claim 53, wherein the data set is accompanied by validity information of said data set, and wherein the security unit transmits to the decoder the information to use or not said validity information for checking the data set.

59. (new): The method according to claim 58, wherein said validity information is of the type of a cyclic redundancy code, a checksum or a code determined with a unidirectional and collision-free function.

60. (new): The method according to claim 53, wherein the control data includes a global check information which is representative of a result of a unidirectional and collision-free function carried out on all or part of a global data set including the received data set or corresponding to the received data set.

61. (new): The method according to claim 60, wherein the control data includes a certificate authenticating the broadcaster of the data set.

62. (new): The method according to claim 60, comprising the steps of calculating periodically, or on request, the global check information, the security unit comparing the result with a reference value of said global check information.

63. (new): The method according to claim 62, wherein the calculation is carried out by the decoder, the result of said calculation being transmitted to the security unit.

64. (new): The method according to claim 62, wherein the calculation is carried out by the security unit, the data set being transmitted from the decoder to the security unit.

65. (new): The method according to claim 62, wherein the periodic calculation is carried out on request from the control center, from the security unit, from a test unit or from one of the means of communication.

66. (new): The method according to claim 62, wherein the result of the comparison is transmitted in a subscription message usual to the functioning of the system.

67. (new): The method according to claim 62, wherein the global check information is transmitted to the control center inside a subscription message usual to the functioning of the system, each message containing only a part of said global check information.

68. (new): The method according to claim 67, wherein the transmission to the control center is carried out in deferred mode, according to a timetable defined in a pseudo-random manner within predefined limits.